OPIS PRZEDMIOTU ZAPYTANIA

Zakup systemu do monitorowania logów oraz zarządzania i monitorowania bezpieczeństwa infrastruktury teleinformatycznej wraz z pracami wdrożeniowymi oraz z wsparciem technicznym

Warszawa, czerwiec 2026

I. Wymagania ogólne

Podstawowe definicje:

1. **dni robocze** – dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy wskazanych w ustawie z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2020 r. poz. 1920) oraz dni przyjętych przez Zamawiającego za dni wolne od pracy, o których Zamawiający powiadomi niezwłocznie Wykonawcę w formie pisemnej z odpowiednim wyprzedzeniem,
2. **godziny robocze** - godziny od 8:15 do 16:15 w dni robocze,
3. **awaria** – stan niesprawności Systemu uniemożliwiający jego prawidłowe funkcjonowanie, występujący nagle i powodujący ich niewłaściwe działanie lub całkowite unieruchomienie,
4. **serwis** – wszelkie usługi świadczone przez Wykonawcę zapewniające prawidłowe funkcjonowanie sprzętu i Systemu do obsługi infolinii w okresie gwarancji,
5. **sprzęt** – fizyczne urządzenia, służące do funkcjonowania Systemu do obsługi infolinii, w tym m. in. serwer/y z oprogramowaniem systemowym,
6. **usterka** – stan, w którym System realizuje zadania, ale sygnalizuje niepoprawne działanie,
7. **System** - kupione i wdrożone oprogramowanie do monitorowania logów oraz zarządzania i monitorowania bezpieczeństwa infrastruktury teleinformatycznej wraz z serwerami i urządzeniami (o ile będą potrzebne),
8. **SIEM** - system centralnego gromadzenia, korelacji i analizy logów oraz zdarzeń bezpieczeństwa z infrastruktury teleinformatycznej,
9. **SOAR** - system służący do automatyzacji procesów obsługi incydentów bezpieczeństwa oraz integracji i koordynacji działań rozproszonych narzędzi ochronnych,
10. **CLM** - system służący do centralnego, automatycznego zarządzania pełnym cyklem życia certyfikatów cyfrowych (np. SSL/TLS) oraz kluczy kryptograficznych,
11. **oprogramowanie** - oprogramowanie niezbędne do zarządzania logami i monitorowania bezpieczeństwa wraz z systemami operacyjnymi, na których jest zainstalowane,
12. **usuwanie awarii lub usterki** – proces przywracania sprawności Systemu do stanu sprzed awarii lub usterki, który będzie liczony od dnia zgłoszenia awarii lub usterki do dnia przywrócenia sprawności działania Systemu,

II. Przedmiot umowy

1. Przedmiotem umowy jest zakup systemu do monitorowania logów oraz zarządzania i monitorowania bezpieczeństwa infrastruktury teleinformatycznej wraz z pracami wdrożeniowymi oraz z wsparciem technicznym.
2. Usługi, o których mowa w pkt. 1 będą świadczone przez Wykonawcę na warunkach i o parametrach technicznych określonych w Opisie przedmiotu zamówienia zwanym dalej „OPZ”.
3. Realizacja przedmiotu Umowy obejmuje wykonanie następujących zadań:
   1) przygotowanie harmonogramu prac uwzględniającego specyfikę organizacji Zamawiającego, koncepcję funkcjonowania Systemu w środowisku Zamawiającego, zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane z określeniem zadań leżących po stronie Wykonawcy i czynnościach leżących po stronie Zamawiającego,

2) przeprowadzenie analizy w zakresie zarządzania logami i monitorowania bezpieczeństwa systemów eksploatowanych przez Zamawiającego w aspekcie wymagań stawianych przez NIS 2 i UKSC,
3) dostarczenie serwerów i urządzeń (o ile będą potrzebne) wraz z oprogramowaniem systemowym,
4) przeprowadzenie prac wdrożeniowych z instruktażem, instalacją i konfiguracją serwerów, urządzeń oraz Systemu wraz z parametryzacją raportów, alertów i komunikatach wysyłanych przez bramkę SMS,
5) wykonanie dokumentacji powykonawczej wdrożonego systemu, o której mowa w pkt 7.
6) zabezpieczenie świadczenia usługi gwarancyjnej w zakresie dostarczonych serwerów oraz urządzeń (o ile będą potrzebne),
7) świadczenie wsparcia technicznego w okresie obowiązywania Umowy.

4. Wykonawca będzie świadczył dodatkowe usługi na rzecz Zamawiającego w tym modyfikacje Systemu wynikające ze zgłoszonych potrzeb funkcjonalnych przez Zamawiającego za dodatkowym wynagrodzeniem. Każdorazowo modyfikacje wymagają wdrożenia ich u Zamawiającego. Termin, wynagrodzenie i zakres realizacji dodatkowych usług, w tym modyfikacji Systemu będzie za każdym razem uzgadniany pomiędzy Stronami w formie pisemnej, pod rygorem nieważności.
5. Zamawiający przewiduje w razie potrzeby do 100 roboczogodzin na dodatkowe odpłatne usługi, w tym na modyfikacje Systemu wynikające z dodatkowych potrzeb funkcjonalnych na warunkach określonych w pkt. 6.
6. Strony ustalają, że postępowanie w zakresie dodatkowej usługi, w tym modyfikacja Systemu wykonywana będzie w sposób następujący:
   1) Zamawiający przygotuje merytoryczne założenia do realizacji dodatkowej usługi (np. do modyfikacji Systemu, do dodatkowego instruktażu) i przekaże je w formie pisemnej do Wykonawcy,
   2) Strony uzgodnią w formie pisemnej (mailowo lub za pomocą pism) zakres realizacji dodatkowej usługi oraz termin jej realizacji;
   3) Strony uzgodnią w formie pisemnej (mailowo lub za pomocą pism) liczbę roboczogodzin niezbędnych do realizacji dodatkowej usługi, a następnie Zamawiający przekaże Wykonawcy zamówienie na tej usługi. Usługa, w odniesieniu, do której Strony nie uzgodnią liczby roboczogodzin nie będzie realizowana,
   4) Wykonawca opracuje specyfikację realizacji dodatkowej usługi i przekaże ją w formie pisemnej (mailowo lub za pomocą pisma) Zamawiającemu,
   5) Zamawiający dokona akceptacji przekazanej specyfikacji albo przekaże w formie pisemnej (mailowo lub za pomocą pisma) uwagi i zastrzeżenia do Wykonawcy,
   6) Wykonawca uwzględnia uwagi i zastrzeżenia do specyfikacji i przekazuje ją w formie pisemnej (mailowo lub za pomocą pisma) do Zamawiającego w celu ostatecznej akceptacji,
   7) czynności określone w ppkt 4-6 będą powtarzane aż do uzyskania ostatecznej akceptacji specyfikacji modyfikacji Systemu przez Zamawiającego,
   8) Wykonawca wykona modyfikację Systemu na podstawie zaakceptowanej specyfikacji, o której mowa w ppkt 7,

9) Wykonawca zaktualizuje i przekaże Zamawiającemu dokumentację techniczną, administracyjną i użytkową zgodnie z zakresem wynikającym z modyfikacji. Ostateczny zakres zmian w dokumentacji zostanie uzgodniony z Zamawiającym,
10) Zdalny dostęp ogranicza się do dwóch wskazanych pracowników Wykonawcy.

7. Dokumentacja powykonawcza obejmuje procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym min.:
   1) Dokumentację powdrożeniową Systemu w tym jego konfigurację,
   2) Procedury operacyjne,
   3) Procedury „Disaster Recovery" (jeżeli będzie wymagana).
8. Dokumentacja powykonawcza podlegała będzie procedurze odbioru, na następujących warunkach:
   1) Wykonawca przekaże do akceptacji Zamawiającego drogą elektroniczną Dokumentację powykonawczą, w terminie uzgodnionym w harmonogramie prac jednak nie później niż w ciągu 5 dni roboczych od wdrożenia Systemu,
   2) Zamawiający w terminie nie dłuższym niż 2 dni robocze od dnia dostarczenia przez Wykonawcę Dokumentacji powykonawczej, za pośrednictwem poczty e-mail poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian,
   3) wszystkie uwagi do Dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni robocze od dnia ich przekazania przez Zamawiającego,
   4) Zamawiający w terminie do 2 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionej Dokumentacji powykonawczej, za pośrednictwem poczty e-mail poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian,
   5) w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego (3 dniowego) terminu dostarczenia Dokumentacji powykonawczej. W przypadku, jeżeli Wykonawca nie dostarczy Dokumentacji powykonawczej, w terminie wskazanym przez Zamawiającego, Zamawiający będzie miał prawo naliczenia kar umownych,
   6) potwierdzeniem odbioru zaakceptowanej przez Zamawiającego Dokumentacji powykonawczej będzie podpisany bez zastrzeżeń Protokół odbioru, w którym będzie umieszczona informacja o odbiorze jakościowym Dokumentacji powykonawczej,
   7) zaakceptowana Dokumentacja powykonawcza zostanie przekazana Zamawiającemu w formie papierowej w 2 egzemplarzach oraz w formie elektronicznej, w postaci plików do edycji i PDF.
9. Wykonawca przygotuje procedury operacyjne w zakresie min:
   1) Wyłączenia Systemu,
   2) Włączenia Systemu,
   3) Zabezpieczeniem systemu,
   4) Odtwarzaniem systemu z kopii zapasowej.

III. Parametry funkcjonalne i techniczne jakie musi spełniać System

W dalszej części dokumentu przedstawione zostały minimalne wymagania do Systemu, które muszą zostać spełnione.

WYMAGANIA WSPÓLNE

ID	Wymagania techniczno-funkcjonalne
1	System musi posiadać wbudowane i konfigurowalne szablony raportów i mechanizmy zgłaszania/sygnalizowania incydentów zgodne z wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC) oraz wymogami raportowania do właściwego CSIRT (CERT Polska / CSIRT GOV), w tym generowanie raportów wstępnych w terminie 24 godzin i raportów końcowych w terminie 72 godzin od wykrycia incydentu
2	System musi pozwalać na dowolne tworzenie, modyfikowanie i przestawianie widżetów graficznych na pulpitach w celu budowania dedykowanych widoków dla operatorów SOC/IT.
3	System musi posiadać wbudowane lub/i konfigurowalne szablony raportów i pulpity nawigacyjne wspomagające weryfikację zgodności z: • RODO (GDPR) — w tym wykrywanie i raportowanie naruszeń ochrony danych osobowych, • Dyrektywą NIS2 oraz polską Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC), • ISO/IEC 27001:2022.
4	System musi umożliwiać konfigurację automatycznego, cyklicznego generowania raportów i wysyłania ich pocztą elektroniczną lub przez API do wskazanych odbiorców przy spełnieniu określonych warunków.
5	System musi spełniać poniższe minimalne wymagania wydajnościowe w środowisku docelowym Zamawiającego (około 40 serwerów fizycznych i wirtualnych, środowisko mieszane Windows/Linux oraz około 200 urządzeń sieciowych).
6	System musi udostępniać wbudowany panel monitorowania własnej wydajności i zdrowia (health dashboard), umożliwiający administratorowi bieżącą obserwację parametrów: obciążenie CPU/RAM, queue depth, opóźnienie indeksowania, liczba odrzuconych zdarzeń (dropped events).
7	System musi umożliwiać instalację na serwerze z systemem operacyjnym Linux (RHEL 8+, AlmaLinux 9+, Ubuntu 22.04+) lub Microsoft Windows Server 2022+.
8	System musi być dostępny przez przeglądarkę internetową — co najmniej Chrome, Firefox i przeglądarki oparte na silniku Chromium — bez instalacji dodatkowych wtyczek po stronie klienta.
9	System musi wspierać dostęp przez HTTPS z możliwością zmiany domyślnego portu nasłuchiwania.
10	System musi działać w oparciu o bazę danych klasy relacyjnej (PostgreSQL lub Microsoft SQL Server) lub dokumentowej — w wersji aktywnie wspieranej przez producenta.
11	System musi być skalowalny horyzontalnie — możliwość dołożenia węzłów wykonawczych (worker nodes) bez przerwy w działaniu.

12	System musi zapewniać ciągłość działania — brak single point of failure dla komponentów krytycznych (orkiestrator, baza danych). Dopuszcza się architekturę aktywny-pasywny z automatycznym przełączeniem.
13	System musi umożliwiać tworzenie niestandardowych ról i uprawnień użytkowników
14	System musi wspierać uwierzytelnianie użytkowników przez Active Directory (LDAP/LDAPS) oraz serwer RADIUS. Musi obsługiwać uwierzytelnianie wieloskładnikowe (MFA) dla kont administracyjnych.
15	System musi szyfrować komunikację wewnętrzną i zewnętrzną z użyciem TLS 1.2 lub TLS 1.3. Wszystkie dane w spoczynku (baza danych, logi, artefakty incydentów) muszą być szyfrowane lub system musi wspierać szyfrowanie na poziomie systemu plików.
16	System musi posiadać pełny audyt log działań użytkowników i automatyzacji — kto, kiedy, jaką akcję wykonał, z jakim wynikiem. Audyt log musi być niemodyfikowalny.
17	System musi umożliwiać wysyłanie powiadomień przez: email (SMTP), SMS (przez bramkę SMS z REST API lub Webhook), Microsoft Teams lub równoważny komunikator, SNMP Trap.
18	System musi zapewnić bezproblemową współpracę z bramką SMS Zamawiającego – SMSEagle typ: NXS9750v4 4G lub jeżeli jest to niemożliwe Wykonawca w ramach dostarczonego systemu musi dostarczyć Zamawiającemu inną bramkę SMS z wykupionym wsparciem technicznym na okres 4 lat z naprawą awarii urządzenia do 2 dni roboczych. Zewnętrzna bramka SMS musi udostępniać interfejs REST API lub mechanizm Webhook (HTTP/HTTPS POST z konfigurowalnym payloadem JSON/XML)
19	System musi umożliwiać eksport raportów i danych incydentów do formatów: min. PDF, CSV, JSON.
20	System musi posiadać wbudowany mechanizm generowania dokumentacji po incydentalnej (post-incident report / RCA) na podstawie osi czasu incydentu, wykonanych akcji i ich wyników.
21	System musi posiadać możliwość integracji użytkowników aplikacji z kontami w Active Directory
22	Wszystkie komponenty, moduły Systemu powinny pochodzić od jednego producenta
23	Zamawiający dopuszcza sytuację, w której poszczególne funkcjonalności, komponenty Systemu będą umieszczone w innych modułach niż określił to Zamawiający
24	System powinien zawierać następujące moduły zaszyte w oprogramowaniu: moduł UEBA (User and Entity Behavior Analytics) i ewentualnie dodatkowo moduł ATA

	(Advanced Threat Analytics).
25	System powinien pozwalać na jednokrotne logowanie podczas korzystania z wymienionych modułów.
26	System powinien integrować wymienione moduły w jeden interfejs użytkownika.
27	System powinien zawierać raporty „Compliance” dla wszystkich zintegrowanych aplikacji z poziomu panelu użytkownika

MODUŁ 1 Moduł analizy logów (SIEM)

ID	Wymagania techniczno-funkcjonalne
1	**Wymagania Architektoniczne i Integracyjne**
1.1	Moduł analizy logów musi stanowić centralny punkt Systemu i posiadać udokumentowane API (REST/JSON) oraz obsługiwać standardowe mechanizmy wymiany danych, w tym co najmniej: Webhook (min. HTTP/HTTPS POST z konfigurowalnym payloadem JSON/XML), Syslog (RFC 5424), CEF (Common Event Format).
1.2	Moduł analizy logów musi natywnie (lub poprzez API/Webhook) integrować się z systemami klasy ITSM (Helpdesk) w celu automatycznego generowania zgłoszeń i incydentów bezpieczeństwa na podstawie wykrytych alertów krytycznych. Integracja musi być dwukierunkowa — system musi umożliwiać odczyt statusu zgłoszenia z systemu ITSM.
1.3	Moduł analizy logów musi posiadać wbudowaną (lub dostarczoną w pakiecie) analityczną bazę danych. Baza danych musi być w wersji aktywnie wspieranej przez producenta.
1.4	Moduł analizy logów musi wspierać mechanizmy Security Hardeningu, w tym co najmniej: szyfrowanie komunikacji wewnętrznej TLS 1.2/1.3, wymuszanie silnych haseł, uwierzytelnianie wieloskładnikowe (MFA) dla administratorów, kontrolę dostępu opartą na rolach (RBAC), audytowanie działań administratorów.
1.5	Moduł analizy logów musi wspierać architekturę zapewniającą jego ciągłość działania — w przypadku awarii pojedynczego węzła system musi kontynuować zbieranie i przetwarzanie logów (brak single point of failure dla komponentów krytycznych). Dopuszcza się architekturę klastrową lub aktywny-pasywny tryb pracy z automatycznym przełączeniem.
1.6	Moduł analizy logów musi być skalowalny horyzontalnie — możliwość dołożenia węzłów przetwarzających lub składowania danych bez przerwy w działaniu i bez utraty danych.
1.7	Moduł analizy logów musi umożliwiać pełne działanie w środowisku bez stałego dostępu do Internetu (tryb air-gapped / offline), w tym aktualizację reguł detekcyjnych, sygnatur i baz podatności w trybie offline poprzez import z nośnika lub serwera pośredniczącego.
1.8	Moduł analizy logów musi posiadać funkcjonalność raportowania i audytowania

	integralności plików.
1.9	Moduł analizy logów musi pozwalać na grupowanie Hostów w celu wdrożenia zasad parsowania logów.
1.10	Moduł analizy logów musi umożliwiać planowe wykonywanie raportów.
1.11	Moduł analizy logów powinien posiadać raporty typu PUMA.
1.12	Moduł analizy logów musi umożliwiać wykonywanie analiz trendów oraz analiz bezpieczeństwa w oparciu o wizualizację zmian wolumenu zdarzeń w czasie, porównywanie okresów historycznych (np. tydzień do tygodnia) oraz automatyczne wykrywanie anomalii statystycznych.
1.13	Moduł analizy logów musi umożliwiać wykonanie polecenia/akcji w przypadku alertów.
2	**Zbieranie logów i obsługiwanie źródeł zdarzeń**
2.1	Moduł analizy logów musi wspierać zarówno bezagentowe zbieranie logów (Syslog UDP/TCP, WMI, WinRM, SNMP Trap, CEF, LEEF, REST API), jak i zbieranie oparte na lekkich agentach instalowanych na systemach końcowych, w celu ominięcia problemów z NAT/Firewall oraz zapewnienia buforowania zdarzeń lokalnie przez minimum 48 godzin w przypadku braku połączenia z serwerem centralnym, z automatycznym przesłaniem zaległych danych po przywróceniu łączności.
2.2	Moduł analizy logów musi zapewniać możliwość zbierania, parsowania i normalizacji danych ze wskazanych źródeł zdarzeń (np. systemy operacyjne, urządzenia sieciowe, systemy backupowe, systemy wirtualizacji), w sposób umożliwiający ich dalszą analizę w tym korelację. Realizacja może odbywać się: • poprzez wbudowane parsery, • poprzez dostarczone konektory producenta, • poprzez mechanizmy integracyjne (API, Syslog, agent), • lub poprzez konfigurowalne mechanizmy parsowania (np. regex, mapowanie pól).
2.3	Zamawiający dopuszcza, aby obsługa wymienionych systemów w pkt 2.4 była realizowana poprzez integrację, o ile nie wymaga ona tworzenia niestandardowego oprogramowania poza dostarczonym rozwiązaniem.
2.4	Moduł analizy logów musi zapewniać możliwość zbierania, parsowania i normalizacji danych, pulpity nawigacyjne i reguły analizy dla środowiska Zamawiającego, w tym minimum dla: • Systemów serwerowych min. Microsoft Windows Server 2016, 2019, 2022, 2025 oraz min. stacji roboczych Windows 10/11. • Usługi katalogowej Active Directory (min. logowania, blokady kont, zmiany GPO, zmiany uprawnień, tworzenie/usuwanie kont). • Systemów z rodziny Linux: min. Red Hat Enterprise Linux, Oracle Linux, Debian, Ubuntu, AlmaLinux — we wszystkich wersjach aktywnie wspieranych przez producentów. • Urządzeń brzegowych i zapór sieciowych min. Fortinet FortiGate (obsługa logów przez Syslog oraz FortiGate API). • Infrastruktury wirtualizacyjnej: min.VMware vSphere/vCenter/ESXi, Microsoft Hyper-V, Proxmox/XCP-NG.

	• Serwerów WWW: minimum Microsoft IIS, Apache HTTP Server, Nginx. • Serwerów baz danych: min. Microsoft SQL Server, PostgreSQL, MySQL/MariaDB, Oracle Database (wersja 12c i nowsze). • Systemów kopii zapasowych — w tym zbieranie alertów o nieudanych lub niekompletnych zadaniach backup (min. Veeam Backup & Replication, Commvault), co stanowi element monitorowania ciągłości działania wymaganego przez NIS2. • Serwerów DNS — zbieranie i analiza zapytań DNS w celu wykrywania technik DNS tunneling, komunikacji C2 oraz data exfiltration przez protokół DNS. • Serwerów DHCP — korelacja przydziałów adresów IP z nazwami hostów i znacznikami czasu, umożliwiająca rzetelny audyt aktywności sieciowej. • Systemów uwierzytelniania MFA (np. Microsoft ADFS, privacyIDEA, Duo Security) lub równoważnych — zbieranie zdarzeń uwierzytelniania wieloskładnikowego.
2.5	Moduł analizy logów musi pozwalać na importowanie historycznych plików logów (płaskie pliki .log, .csv, .txt) oraz ich parsowanie i indeksowanie z możliwością wskazania formatu i strefy czasowej.
2.6	Moduł analizy logów musi posiadać graficzny, interaktywny kreator pozwalający na tworzenie własnych ekstraktorów danych dla niestandardowych logów aplikacji wewnętrznych, oparty co najmniej na wyrażeniach regularnych (Regex) lub wizualnym mapowaniu pól.
3	**Moduł analizy logów - Korelacja Zdarzeń i Analiza Zagrożeń**
3.1	Moduł analizy logów musi pełnić rolę agregatora informacji o bezpieczeństwie i pozwalać na korelację zdarzeń z wielu niezależnych źródeł w czasie rzeczywistym.
3.2	Moduł analizy logów musi posiadać wbudowaną bazę predefiniowanych reguł korelacyjnych mapujących zachowania na techniki ataku zgodnie z matrycą MITRE ATT&CK (w wersji aktualnej w dniu dostawy), pozwalającą m.in. na: a) wykrywanie aktywności charakterystycznej dla oprogramowania ransomware (masowe zmiany rozszerzeń plików, kasowanie kopii cieniowych VSS, szyfrowanie w krótkim czasie). b) wykrywanie prób ataków na aplikacje webowe (SQL Injection, XSS, skanowanie ścieżek, wykrywanie skanerów podatności). c) wykrywanie anomalii sieciowych i wolumetrycznych (skanowanie portów, potencjalne ataki DoS/DDoS, komunikacja z adresami z list IoC). d) wykrywanie technik lateral movement (Pass-the-Hash, Pass-the-Ticket, złośliwe użycie narzędzi administracyjnych PSExec, WMI, PowerShell).
3.3	Moduł analizy logów musi budować dynamiczne linie bazowe (baseline) normalnego zachowania użytkowników i hostów oraz generować alerty przy istotnym odchyleniu od normy (analiza behawioralna / UEBA — User and Entity Behavior Analytics), bez konieczności ręcznego definiowania progów dla każdego zasobu z osobna.
3.4	Moduł analizy logów musi wspierać pobieranie zewnętrznych list wskaźników kompromitacji (IoC) z platform Threat Intelligence ze wsparciem dla standardów STIX

	2.x / TAXII 2.x, a także umożliwiać ręczny import list IoC w formatach CSV i OpenIOC. System musi automatycznie korelować obserwowane zdarzenia z bazą IoC w czasie rzeczywistym (adresy IP, domeny, hasze plików MD5/SHA1/SHA256, sygnatury).
3.5	Moduł analizy logów musi wspierać mechanizmy zarządzania przepływem pracy incydentu (Incident Workflow) — od wykrycia, przez przypisanie analityka, eskalację, po zamknięcie — samodzielnie lub poprzez dwukierunkową integrację z usługami ITSM.
3.6	Moduł analizy logów musi posiadać wbudowany mechanizm automatycznej reakcji na zdarzenia (playbooki / response actions), umożliwiający co najmniej: blokadę konta użytkownika w Active Directory, wysłanie powiadomienia email/SMS, wywołanie Webhooka — jako akcje wyzwalane automatycznie przez regułę lub ręcznie przez operatora jednym kliknięciem.
4	**Monitorowanie Integralności i Audyt Systemowy**
4.1	Moduł analizy logów (bezpośrednio lub poprzez dostarczonych agentów) musi realizować funkcję Monitorowania Integralności Plików (FIM — File Integrity Monitoring) dla krytycznych ścieżek systemowych w systemach Windows i Linux. Monitorowanie musi obejmować co najmniej: tworzenie, modyfikację, usunięcie pliku/katalogu, zmianę uprawnień, zmianę właściciela oraz zmianę zawartości (wykrywanie przez hash kryptograficzny).
4.2	Moduł analizy logów musi pozwalać na monitorowanie i audytowanie zmian w Rejestrze systemowym Windows (wskazane klucze i wartości rejestru).
4.3	Moduł analizy logów musi korelować logi z urządzeń sieciowych (VPN, firewall) z logami systemowymi w celu identyfikacji anomalii behawioralnych, takich jak np.: niemożliwa podróż użytkownika (Impossible Travel), współdzielenie poświadczeń, logowanie z nieoczekiwanej lokalizacji lub o nieoczekiwanej porze.
4.4	Moduł analizy logów musi dostarczać predefiniowane scenariusze audytowe skupione na monitorowaniu użytkowników uprzywilejowanych (administratorów lokalnych, adminów domeny AD) oraz śledzeniu ich operacji na kluczowych serwerach.
4.5	Moduł analizy logów musi monitorować zdarzenia związane z infrastrukturą wirtualizacyjną: tworzenie i usuwanie maszyn wirtualnych, eksport VM, modyfikacje snapshotów, zmiany konfiguracji hypervisora.
5	**Raportowanie, Wyszukiwanie i Zgodność (Compliance)**
5.1	Moduł analizy logów musi zapewniać graficzny interfejs (GUI) umożliwiający szybkie przeszukiwanie surowych logów (Full-text search), filtrowanie po wyodrębnionych polach, budowanie zapytań bez znajomości języka programowania oraz zapisywanie zapytań jako alerty lub widżety na pulpitach nawigacyjnych.
5.2	Moduł analizy logów musi archiwizować logi w sposób gwarantujący ich nienaruszalność i integralność przed modyfikacją — poprzez kryptograficzne hashowanie archiwów (co najmniej SHA-256) lub mechanizm WORM (Write Once Read Many). Zamawiający dopuszcza realizację wymagania integralności przez integrację z zewnętrznym systemem storage (np. macierzą dyskową z funkcją SnapLock/WORM).

5.3	Raporty generowane automatycznie muszą być opatrzone metadanymi umożliwiającymi weryfikację ich autentyczności: data i czas generowania, wersja systemu, identyfikator żądania, skrót kryptograficzny treści raportu.
5.4	Moduł analizy logów musi umożliwiać eksport surowych logów oraz wyników zapytań do formatów: CSV, JSON, PDF. System musi umożliwiać przesyłanie danych do systemów zewnętrznych przez API (np. do systemu ITSM lub archiwum).
6	**Wymagania wydajnościowe i operacyjne**
6.1	System musi spełniać poniższe minimalne wymagania wydajnościowe w środowisku docelowym Zamawiającego (około 40 serwerów fizycznych i wirtualnych, środowisko mieszane Windows/Linux oraz około 200 urządzeń sieciowych): • Minimalna przepustowość (EPS) - 3000 EPS ciągłe / 7500 EPS szczytowe • Czas odpowiedzi — zapytanie 24h Full-text search po surowych logach - ≤ 15 sekund • Czas odpowiedzi — zapytanie 90 dni - ≤ 120 sekund • Jednocześni użytkownicy GUI - Analitycy SOC / administratorzy - ≥ 4 bez degradacji czasu odpowiedzi interfejsu powyżej wartości progowych określonych dla zapytań w niniejszej tabeli • Retencja hot storage - Pełne przeszukiwanie i korelacja - ≥ 90 dni • Retencja archiwum (cold) - Zgodność z NIS2 / RODO - ≥ 12 miesięcy • Buforowanie agenta (offline) - Przy braku połączenia z serwerem - ≥ 48 godzin
6.2	Realizacja powyższych funkcji musi odbywać się przynajmniej przez jeden z następujących mechanizmów: • natywne mechanizmy systemu, • dedykowane agenty, • integrację z usługami katalogowymi, lub mechanizmy parsowania logów zdarzeń systemowych.

MODUŁ 2 Moduł audytu AD

ID	Wymagania techniczno-funkcjonalne
1	**Audyt i monitorowanie środowiska Active Directory (AD)**
1.1	Moduł audytu AD musi zapewniać zaawansowany audyt środowiska Active Directory, obejmujący zbieranie, korelację oraz analizę zdarzeń związanych z uwierzytelnianiem, autoryzacją oraz zmianami w strukturze katalogowej.
1.2	Moduł audytu AD musi umożliwiać monitorowanie co najmniej następujących zdarzeń: • logowania interaktywne i sieciowe (udane i nieudane), • blokady i odblokowania kont,

	• zmiany haseł oraz polityk haseł, • tworzenie, modyfikację i usuwanie kont użytkowników oraz grup, • zmiany członkostwa w grupach uprzywilejowanych (np. Domain Admins, Enterprise Admins), • modyfikacje obiektów GPO oraz ich przypisań, • zmiany uprawnień (ACL) do obiektów AD, • operacje na kontrolerach domeny (DC).
1.3	Moduł audytu AD musi umożliwiać wykrywanie i korelację zdarzeń wskazujących na potencjalne nadużycia lub ataki, w tym: • próby brute force i password spraying, • użycie kont uprzywilejowanych poza standardowymi godzinami pracy, • tworzenie nietypowych kont lub eskalację uprawnień, • techniki lateral movement (np. Pass-the-Hash, Pass-the-Ticket), • anomalie logowania (np. „impossible travel", logowanie z nieoczekiwanej lokalizacji lub o nieoczekiwanej porze).
1.4	Moduł audytu AD musi umożliwiać budowanie profili behawioralnych użytkowników i administratorów AD (UEBA) oraz wykrywanie odchyleń od standardowych wzorców aktywności.
1.5	Moduł audytu AD musi zapewniać dedykowane pulpity nawigacyjne (dashboardy) i raporty dla środowiska Active Directory, w tym: • aktywność kont uprzywilejowanych, • zmiany w strukturze katalogowej, • próby nieautoryzowanego dostępu, • zdarzenia krytyczne z punktu widzenia bezpieczeństwa.
1.6	Moduł audytu AD musi umożliwiać powiązanie zdarzeń AD z danymi z innych źródeł (np. VPN, firewall, systemy końcowe) w celu pełnej korelacji incydentów bezpieczeństwa.
1.7	Moduł audytu AD musi zapewniać możliwość generowania raportów audytowych dla środowiska AD wspierających spełnienie wymagań regulacyjnych, w tym w zakresie kontroli dostępu, rozliczalności działań oraz wykrywania incydentów.
1.8	Realizacja powyższych funkcji musi odbywać się przynajmniej przez jeden z następujących mechanizmów: • natywne mechanizmy systemu, • dedykowane agenty, • integrację z usługami katalogowymi, lub mechanizmy parsowania logów zdarzeń systemowych.

MODUŁ 3 Moduł SOAR

ID	Wymagania techniczno-funkcjonalne
1	**Wymagania Architektoniczne i bezpieczeństwo systemu**
1.1	Moduł SOAR musi być wdrażalny w środowisku on-premise, bez wymogu stałego połączenia z chmurą producenta. Wszelkie funkcje podstawowe (playbooki, wykonywanie akcji, zarządzanie incydentami) muszą działać w pełni offline.
2	**Integracje i interoperacyjność** Wymagania tej sekcji są kluczowe dla zapewnienia współpracy modułu SOAR z modułem SIEM oraz z pozostałą infrastruktura IT organizacji. Zamawiający wymaga, aby wszystkie integracje korzystały z udokumentowanych, standardowych protokołów (REST API, Webhook, CEF) — bez zależności od właściwości protokolarnych konkretnego producenta.
2.1	Moduł SOAR musi pobierać alerty i zdarzenia z zewnętrznego systemu SIEM przez REST API lub Webhook (HTTP/HTTPS POST z payloadem JSON). Integracja musi być dwukierunkowa — system musi móc aktualizować status incydentu w SIEM po zakończeniu reakcji.
2.2	Moduł SOAR musi obsługiwać standardowe formaty zdarzeń wejściowych min.: JSON, CEF (Common Event Format), LEEF (Log Event Extended Format), Syslog (RFC 5424).
2.3	Moduł SOAR musi umożliwiać integrację z Active Directory w celu wykonywania akcji: blokada konta użytkownika, odblokowanie konta, wymuszenie zmiany hasła, dodanie/usunięcie z grupy bezpieczeństwa.
2.4	Moduł SOAR musi umożliwiać integrację z zaporami sieciowymi klasy NGFW przez REST API lub SSH w celu wykonywania akcji: blokada adresu IP, blokada domeny, izolacja hosta, modyfikacja reguł ACL.
2.5	Moduł SOAR musi umożliwiać integrację z systemami klasy ITSM/Helpdesk przez REST API lub Webhook w celu automatycznego tworzenia, aktualizacji i zamykania zgłoszeń serwisowych.
2.6	Moduł SOAR musi obsługiwać pobieranie i wzbogacanie danych o zagrożeniach z platform Threat Intelligence przez standardy STIX 2.x / TAXII 2.x oraz import ręczny list IoC w formatach CSV i OpenIOC.
2.7	Moduł SOAR musi umożliwiać integrację z systemami analizy podatności (vulnerability scanners) przez REST API w celu pobierania informacji o podatnościach wykrytych na hostach będących przedmiotem incydentu.
2.8	Moduł SOAR musi posiadać bibliotekę gotowych konektorów (integracji) obejmującą co najmniej: Active Directory, systemy NGFW wiodących producentów, platformy Threat Intelligence, systemy ITSM, systemy analizy

ID	Wymagania techniczno-funkcjonalne
	złośliwego oprogramowania (sandbox). Dostawca musi wskazać pełną listę dostępnych konektorów.
2.9	Moduł SOAR musi udostępniać SDK lub udokumentowane API umożliwiające tworzenie własnych konektorów do systemów nieobsługiwanych out-of-the-box.
3	**Playbooki i automatyzacja**
3.1	Moduł SOAR musi umożliwiać tworzenie, zarzadzanie i wykonywanie playbookow bez konieczności posiadania umiejętności programistycznych przez analityków SOC.
3.2	Moduł SOAR musi posiadać graficzny edytor playbooków (workflow) umożliwiający tworzenie, modyfikację i wizualizację automatycznych procedur reagowania bez znajomości języka programowania (low-code / no-code).
3.3	Moduł SOAR musi umożliwiać tworzenie złożonych scenariuszy reagowania (playbooków), obejmujących logikę warunkową, obsługę błędów, wykonywanie równoległe oraz interakcję z użytkownikiem. Sposób realizacji powyższych funkcji jest dowolny, o ile pozwala na osiągnięcie równoważnego efektu operacyjnego.
3.4	Moduł SOAR musi umożliwiać wersjonowanie playbooków — możliwość powrotu do poprzedniej wersji, porównywanie wersji, oznaczanie wersji jako aktywna/archiwalna.
3.5	Moduł SOAR musi umożliwiać eksport i import playbooków w ustandaryzowanym formacie (JSON lub YAML) w celu przenoszenia między środowiskami (dev/test/prod)
3.6	Moduł SOAR musi posiadać bibliotekę predefiniowanych playbooków obejmującą co najmniej następujące scenariusze: phishing, ransomware, brute force / credential stuffing, nieautoryzowany dostęp uprzywilejowany, wykrycie złośliwego oprogramowania, naruszenie danych osobowych (RODO art. 33).
3.7	Moduł SOAR musi umożliwiać testowanie playbooków w trybie symulacji (dry-run) bez wykonywania rzeczywistych akcji na systemach produkcyjnych.
3.8	Moduł SOAR musi umożliwiać uruchamianie playbooków: automatycznie (wyzwolenie przez alert/regułę), manualnie przez analityka, cyklicznie według harmonogramu.
3.9	Moduł SOAR musi obsługiwać parametryzację playbooków — możliwość przekazywania zmiennych wejściowych (np. adres IP, nazwa użytkownika, hash pliku) jako parametrów uruchomienia.
4	**Zarządzanie incydentami bezpieczeństwa (SOAR)**
4.1	Moduł SOAR musi posiadać graficzny interfejs zarządzania incydentami

ID	Wymagania techniczno-funkcjonalne
	bezpieczeństwa umożliwiający: tworzenie incydentów (manualnie lub automatycznie z alertu SIEM), przypisywanie analityków do incydentów, ustawianie priorytetu i statusu incydentu, śledzenie postępu w obsłudze incydentu.
4.2	Moduł SOAR musi umożliwiać automatyczne tworzenie incydentów na podstawie alertów przychodzących z SIEM według konfigurowalnych reguł (np. typ alertu, poziom krytyczności, źródło, czas wystąpienia).
4.3	Moduł SOAR musi umożliwiać grupowanie powiązanych alertów w jeden incydent (alert deduplication / grouping) na podstawie konfigurowalnych kryteriów: wspólny host, wspólny użytkownik, wspólny adres IP, przedział czasowy.
4.4	Moduł SOAR musi umożliwiać wzbogacanie incydentów o kontekst zewnętrzny: dane WHOIS, geolokalizacja IP, reputacja IP/domeny/hasha pliku z baz Threat Intelligence, informacje o podatnościach hosta.
4.5	Moduł SOAR musi umożliwiać dołączanie artefaktów do incydentu: pliki (logi, zrzuty pamięci, próbki złośliwego oprogramowania), zrzuty ekranu, notatki analityczne, wyniki zewnętrznych analiz.
4.6	Moduł SOAR musi rejestrować pełną oś czasu (timeline) każdego incydentu: wszystkie wykonane akcje manualne i automatyczne, zmiany statusu, komentarze analityków, wyniki akcji — z dokładnymi znacznikami czasu.
4.7	Moduł SOAR musi umożliwiać eskalację incydentu do wyższego poziomu analityka lub kierownictwa z automatycznym powiadomieniem np. pocztą elektroniczną lub przez API do wskazanych odbiorców.
4.8	Moduł SOAR musi umożliwiać współpracę wielu analityków nad tym samym incydentem jednocześnie (komentarze, przypisywanie zadań, podgląd aktywności innych użytkowników w czasie rzeczywistym).
4.9	Moduł SOAR musi obsługiwać pełny cykl życia incydentu: Nowy → W toku → Oczekuje na akcję → Zamknięty → Ponownie otwarty. Statusy muszą być konfigurowalne.
4.10	Moduł SOAR musi posiadać mechanizm SLA dla incydentów — konfigurowalny czas reakcji i czas rozwiązania per poziom krytyczności, z alertami przy przekroczeniu SLA.
5	**Raportowanie, metryki i zgodność**
5.1	Moduł SOAR musi posiadać graficzny dashboard z widokiem w czasie rzeczywistym: liczba aktywnych incydentów per status i krytyczność, wskaźniki MTTR (Mean Time To Respond) i MTTD (Mean Time To Detect), obciążenie analityków, status wykonywanych playbooków.

ID	Wymagania techniczno-funkcjonalne
5.2	Moduł SOAR musi umożliwiać tworzenie niestandardowych dashboardów i widżetów graficznych (wykresy, tabele, mapy cieplne) dostosowanych do roli użytkownika (np. analityk SOC, kierownik, CISO).
5.3	Moduł SOAR musi posiadać wbudowane raporty zgodności i operacyjne, w tym co najmniej: raport aktywności analityków, raport czasu reakcji na incydenty (SLA compliance), raport najczęstszych typów incydentów, raport skuteczności playbooków.
5.4	Moduł SOAR musi umożliwiać analizę trendów dla zdarzeń historycznych: zmiany wolumenu incydentów w czasie, powtarzające się typy ataków, skuteczność wdrożonych środków zaradczych
6	**Wymagania operacyjne i API**
6.1	Moduł SOAR musi posiadać dokumentowane REST API umożliwiające zewnętrznym systemom: tworzenie incydentów, pobieranie statusu incydentów, wyzwalanie playbooków, pobieranie wyników akcji. API musi być wersjonowane i opisane w standardzie OpenAPI (Swagger).
6.2	Moduł SOAR musi obsługiwać Webhook jako mechanizm wyzwalający — możliwość uruchomienia playbooka przez zewnętrzne wywołanie HTTP/HTTPS POST z payloadem JSON.
6.3	Moduł SOAR musi posiadać mechanizm kolejkowania zadań zapewniający że żadna akcja automatyczna nie zostanie utracona w przypadku chwilowej niedostępności systemu docelowego.
6.4	Moduł SOAR musi umożliwiać pełne działanie w środowisku bez stałego dostępu do Internetu (tryb air-gapped / offline). Aktualizacje biblioteki konektorów i playbooków muszą być możliwe w trybie offline np. przez import z nośnika.
6.5	Moduł SOAR musi umożliwiać monitorowanie własnej wydajności i zdrowia (health dashboard): statusu węzłów, długości kolejki zadań, czasu wykonania playbooków, błędów integracji.
6.6	Moduł SOAR musi umożliwiać konfigurację limitów wykonań playbooków (throttling) w celu ochrony systemów docelowych przed przeciążeniem akcjami automatycznymi.

MODUŁ 4 Moduł CLM

1	**Audyt i zarządzanie kluczami kryptograficznymi (SSH) oraz certyfikatami cyfrowymi (SSL/TLS)**

1.1	Moduł CLM musi posiadać wbudowane mechanizmy automatycznego wykrywania (Discovery) lub umożliwiać integrację z narzędziami służącymi do wykrywania, inwentaryzacji, monitorowania i audytu kluczy SSH oraz certyfikatów SSL/TLS w infrastrukturze Zamawiającego. Mechanizm wykrywania musi umożliwiać: • skanowanie sieciowe (aktywne): automatyczne przeszukiwanie wskazanych podsieci IP oraz portów (np. 443, 8443 itp.) w celu identyfikacji uruchomionych usług SSL/TLS i pobrania ich certyfikatów, • skanowanie systemów i urządzeń (host-based): skanowanie systemów operacyjnych (Windows, Linux/Unix) oraz systemów plików w celu odnalezienia przechowywanych kluczy SSH (publicznych i prywatnych) oraz certyfikatów w lokalnych magazynach (np. magazyn certyfikatów Windows, Keystores Java, katalogi .ssh).
1.2	W zakresie kluczy SSH system musi umożliwiać: • identyfikację i inwentaryzację kluczy publicznych i prywatnych w systemach Linux/Unix, • wykrywanie kluczy nieautoryzowanych, przestarzałych lub niespełniających polityk bezpieczeństwa, • identyfikację współdzielonych kluczy oraz powiązań między użytkownikami i systemami, • automatyczne inicjowanie działań naprawczych (np. usunięcie klucza, rotacja, zgłoszenie incydentu), • powiązanie kluczy z użytkownikami i incydentami bezpieczeństwa.
1.3	W zakresie certyfikatów SSL/TLS system musi umożliwiać: • inwentaryzację certyfikatów wykorzystywanych w infrastrukturze (serwery, aplikacje, urządzenia sieciowe), • monitorowanie dat ważności certyfikatów oraz generowanie alertów o zbliżającym się wygaśnięciu, • identyfikację certyfikatów niespełniających polityk bezpieczeństwa (np. słabe algorytmy, nieznane CA), • wykrywanie nieautoryzowanych lub nieznanych certyfikatów, • automatyczne inicjowanie działań (np. zgłoszenie, rotacja, wycofanie certyfikatu).
1.4	Moduł CLM musi umożliwiać powiązanie informacji o kluczach SSH i certyfikatach SSL/TLS z incydentami bezpieczeństwa obsługiwanymi przez SOAR oraz wykorzystywanie tych danych w playbookach.
1.5	Moduł CLM musi umożliwiać tworzenie playbooków automatyzujących procesy związane z: • rotacją kluczy SSH, • odnawianiem certyfikatów, • reagowaniem na wykrycie nieautoryzowanego klucza lub certyfikatu,

	• eskalacją incydentów związanych z naruszeniem polityk kryptograficznych.
1.6	Moduł CLM musi umożliwiać generowanie raportów audytowych obejmujących: • stan kluczy SSH, • stan certyfikatów SSL/TLS, • wykryte niezgodności z polityką bezpieczeństwa, • historię działań naprawczych.
1.7	Realizacja powyższych funkcji może odbywać się poprzez: • natywne funkcjonalności systemu, • integrację z zewnętrznymi narzędziami klasy PAM, PKI, Certificate Management lub SSH Key Management, • lub poprzez dedykowane konektory i API.
1.8	Zamawiający dopuszcza rozwiązania równoważne funkcjonalnie, o ile zapewniają pełną widoczność (inwentaryzację), audyt oraz możliwość reakcji na zdarzenia związane z zarządzaniem kluczami i certyfikatami.

IV. Gwarancja i wsparcie techniczne

1. Warunki gwarancji na dostarczone serwery, urządzenia:
   1) Okres gwarancji na dostarczone, zainstalowane i skonfigurowane serwery, urządzenia, wynosi …. miesięcy (w zależności od złożonej oferty) od dnia ich protokolarnego odbioru,
   2) Okres gwarancji, o którym mowa w ppkt 1 będzie liczony od daty podpisania przez Zamawiającego, bez zastrzeżeń, Protokołu odbioru,
   3) Wykonawca odpowiada za prawidłową obsługę zgłoszeń gwarancyjnych, w tym za dotrzymanie terminów napraw serwerów, urządzeń określonych w ppkt 5 i 7,
   4) Wykonawca w terminie do 5 dni od daty dostawy serwerów, urządzenia do Zamawiającego zobowiązany będzie dostarczyć prawidłowo wystawioną kartę gwarancyjną, w której zamieści informacje o nazwie, adresie i telefonie podmiotu wykonującego naprawy gwarancyjne,
   5) Gwarantowany czas naprawy dostarczonych serwerów, urządzeń przez Wykonawcę, wynosi do …. dni roboczych (w zależności od złożonej oferty przez Wykonawcę) od dnia zgłoszenia awarii oraz do …. dni roboczych (w zależności od złożonej oferty przez Wykonawcę) od dnia zgłoszenia usterki realizowany w miejscu instalacji serwera, urządzenia.

      Wykonawca zapewni możliwość przyjmowania zgłoszeń o usterkach i awariach w działaniu serwerów, urządzeń w dni robocze w godz. 8:15-16:15. Zamawiający będzie

dokonywał zgłoszenia drogą elektroniczną lub pisemnie. Zgłoszenia o usterkach i awariach w działaniu serwerów, urządzeń doręczone Wykonawcy w dni robocze po godz. 16:15 lub w dni ustawowo wolne od pracy traktowane będą jako zgłoszenia otrzymane o godz. 8:15 kolejnego dnia roboczego,

6) W przypadku gdy naprawa serwera, urządzenia nie będzie możliwa w terminach określonych w ppkt. 5, na żądanie Zamawiającego, Wykonawca następnego dnia roboczego – na czas naprawy – dostarczy, na własny koszt serwer, urządzenie o parametrach nie gorszych od posiadanego przez Zamawiającego, a także dokona jego instalacji i konfiguracji celem zapewnienia poprawnej pracy,
7) Wykonawca zobowiązany będzie do wymiany serwera, urządzenia na nowe w terminie do 5 dni roboczych, od dnia zgłoszenia przez Zamawiającego takiego żądania w formie pisemnej, w przypadkach:
   a) wystąpienia kolejnej awarii lub usterki serwera, urządzenia, po wcześniejszym wykonaniu 3 napraw serwera, urządzenia,
   b) niewykonania naprawy w terminie do 30 dni,
8) W przypadku wymiany serwera, urządzenia na nowe, bieg okresu gwarancji rozpoczyna się na nowo, od dnia jego wymiany przez Wykonawcę, potwierdzonej protokołem odbioru przez Strony Umowy bez zastrzeżeń,
9) Wykonawca w terminie do 5 dni od daty dostawy nowego serwera, urządzenia do Zamawiającego zobowiązany będzie dostarczyć prawidłowo wystawioną nową kartę gwarancyjną, w której zamieści informacje o nazwie, adresie i telefonie podmiotu wykonującego naprawy gwarancyjne,
10) W przypadku awarii dysków twardych uszkodzone dyski pozostają u Zamawiającego, a w ich miejsce zostaną dostarczone nowe o parametrach nie gorszych od zaoferowanych,
11) W przypadku konieczności wymiany lub naprawy dostarczonego serwera, urządzenia poza siedzibą Zamawiającego dyski twarde pozostają u Zamawiającego,
12) Serwis gwarancyjny obejmuje naprawę serwera, urządzeń przez firmę zajmującą się ich naprawą, posiadającą wykwalifikowanych serwisantów i zaplecze techniczne.

2. W ramach udzielonego wsparcia technicznego Wykonawca:
   1) Wykonawca obejmie wdrożony System wsparciem technicznym. Wsparcie techniczne będzie trwało przez okres … miesięcy *(w zależności od złożonej oferty)* począwszy od dnia protokolarnego odbioru.
   2) W ramach udzielonego wsparcia technicznego Wykonawca:
      a) zapewni koordynatora obsługi wsparcia technicznego, z którym będą prowadzone wszelkie bieżące uzgodnienia w zakresie realizacji napraw wdrożonego Systemu i jego przeglądów,
      b) uruchomi kanał kontaktowy w formie elektronicznej przez stronę www lub za pomocą poczty elektronicznej e-mail, umożliwiający zgłaszanie awarii, usterek i konsultacji,
      c) zapewni realizację wsparcia technicznego w języku polskim,
      d) zapewni pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem wdrożonego Systemu,
      e) zapewni obsługę, poniższych problemów w przypadku ich wystąpienia:

- usuwanie wad konfiguracyjnych Systemu wdrożonego w ramach realizacji umowy,
- przywracanie pełnej funkcjonalności działania wdrożonego Systemu, jeżeli jego awaria w tym niewłaściwe działanie wynika z niewłaściwej instalacji lub niewłaściwej konfiguracji Systemu lub niesprawności serwera, urządzenia.

3) Wykonawca w ramach wsparcia technicznego zobowiązany jest, nie rzadziej niż co 6 miesięcy, przeprowadzić przegląd i strojenie wdrożonego Systemu, w tym ostatni przegląd ma nastąpić w ostatnim miesiącu obowiązywania wsparcia technicznego. W trakcie przeglądu Wykonawca musi:
   a) sprawdzić poprawność funkcjonowania Systemu,
   b) wyjaśnić zaistniałe błędy lub alerty informacyjne,
   c) sprawdzić parametry wydajnościowe środowiska i Systemu,
   d) dokonać niezbędnych optymalizacji.

4) Zakres przeprowadzonych prac, o których mowa w ppkt 3 winien być każdorazowo udokumentowany protokołem. W przypadku konieczności zmiany/aktualizacji Dokumentacji powykonawczej, w wyniku dokonania zmian konfiguracyjnych w trakcie przeglądów, Wykonawca zobowiązany jest dostarczyć zaktualizowaną dokumentację w terminie do …. dni roboczych (w zależności od złożonej oferty przez Wykonawcę) od dnia przeprowadzenia zmian konfiguracyjnych.

5) Usługi wsparcia technicznego w zakresie wdrożonego Systemu, świadczone będą w miejscu instalacji lub za pomocą mechanizmów dostępu zdalnego na następujących warunkach:
   a) zgłoszenie awarii i usterek Systemu będzie możliwe w dni robocze w godzinach 8:15-16:15 przez stronę www wskazaną przez Wykonawcę, lub za pomocą poczty elektronicznej e-mail na adres wskazany przez Wykonawcę;
   b) usunięcie awarii i przywrócenie pełnej funkcjonalności Systemu wykazującego awarię, zostanie wykonane w terminie do …… (w zależności od złożonej oferty) dnia roboczego/dni roboczych od dnia zgłoszenia awarii;
   c) usunięcie usterki i przywrócenie pełnej funkcjonalności Systemu wykazującego usterkę, zostanie wykonane w terminie do …… (w zależności od złożonej oferty) dnia roboczego/dni roboczych od dnia zgłoszenia usterki;
   d) jeżeli w trakcie świadczenia usług wsparcia technicznego okaże się, że całkowite usunięcie awarii, możliwe jest wyłącznie poprzez opracowanie poprawki do oprogramowania, Wykonawca może na piśmie wystąpić do Zamawiającego o zgodę na przesunięcie terminu usunięcia awarii wprowadzając jednocześnie jej obejście. Tymczasowe usunięcie awarii może być realizowane poprzez zmianę parametrów wdrożonego Systemu. Zastosowanie obejścia nie zwalnia Wykonawcy od obowiązku dostarczenia rozwiązania docelowego w zakresie usunięcia awarii i nie może powodować utraty funkcjonalności wdrożonego Systemu. Zamawiający wyraża zgodę na przesunięcie terminu usunięcia awarii za pośrednictwem poczty elektronicznej e-mail, na okres do czasu opracowania poprawki przez producenta oprogramowania jednak nie dłużej niż 30 dni przez datą zakończenia Umowy;

e) wszelkie koszty związane z świadczeniem wsparcia technicznego w tym usuwaniem awarii, usterek włączając w to koszt podróży z i do siedziby Zamawiającego ponosi Wykonawca;
f) dopuszcza się, w uzgodnieniu z Zamawiającym, połączenie zdalne do sieci informatycznej, przez system zdalnego dostępu Zamawiającego, którym zarządzają wyznaczeni administratorzy Zamawiającego;
g) usunięcie awarii, usterki będzie każdorazowo potwierdzone Protokołem wykonania naprawy;
h) w przypadku nieterminowego usuwania awarii, usterki Zamawiający zastrzega sobie prawo do naliczenia kar umownych za zwłokę i potrącania ich z wynagrodzenia za realizowane wsparcie techniczne;
i) w przypadku, jeżeli Wykonawca nie usunie awarii, usterki w okresie dłuższym niż 10 dni roboczych licząc od dnia zgłoszenia awarii, usterki z zastrzeżeniem lit. d, Zamawiający może dokonać czynności naprawy we własnym zakresie lub zlecić jej wykonanie podmiotowi trzeciemu, a kosztami obciążyć Wykonawcę.

6) Zamawiający ma prawo dokonywania rozbudowy wdrożonego Systemu powstałego w trakcie realizacji Umowy o nowe funkcjonalności po poinformowaniu o zmianach Wykonawcy. W przypadku uwag do zaproponowanego przez Zamawiającego rozwiązania Wykonawca ma obowiązek w ciągu pięciu dni roboczych odnieść się do zmian, które mają być wprowadzone.
7) Wykonawca zobowiązuję się do świadczenia usług wsparcia technicznego w sposób zapobiegający utracie lub nieuprawnionej modyfikacji danych lub nieuprawnionemu dostępowi do danych, w tym także tych, do których będzie miał dostęp w trakcie wykonywania usług. W przypadku gdy wykonanie danej czynności przez Wykonawcę lub przez Zamawiającego w oparciu o rekomendacje Wykonawcy wiąże się z ryzkiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do wykonania takiej czynności lub z chwilą przekazania takiej rekomendacji Zamawiającemu.
8) Wykonawca odpowiada za prawidłową obsługę zgłoszeń serwisowych, w tym za dotrzymanie terminów napraw Systemu określonych w ppkt. 5 lit. b - c, pkt. 1 ppkt 5 - 7.
9) Wykonawca zapewni możliwość przyjmowania zgłoszeń o usterkach i awariach w działaniu Systemu w dni robocze w godz. 8:15-16:15. Zamawiający będzie dokonywał zgłoszenia drogą elektroniczną lub pisemnie. Zgłoszenia o usterkach i awariach w działaniu Systemu doręczone Wykonawcy w dni robocze po godz. 16:15 lub w dni ustawowo wolne od pracy traktowane będą jako zgłoszenia otrzymane o godz. 8:15 kolejnego dnia roboczego,
10) W okresie wsparcia technicznego Wykonawca zapewnia Zamawiającemu wsparcie w postaci konsultacji telefonicznych lub w siedzibie Zamawiającego w zakresie funkcjonowania Systemu oraz zapewni, na żądanie Zamawiającego, pomoc w instalacji udostępnianych przez producenta Systemu, serwerów, urządzeń uaktualnień i poprawek. Zamawiający nie jest zobowiązany do ponoszenia dodatkowych kosztów z tego tytułu,
11) Wykonawca zapewni wsparcie konsultacyjne w zakresie eksploatowanego Systemu na okres obowiązywania umowy, drogą telefoniczną i e-mailową na podany w umowie nr telefonu i adres e-mail,

12) W przypadku nieterminowego usuwania awarii, usterki, o których mowa w pkt. 1 ppkt 5, wymiany serwera, urządzenia o których mowa w pkt. 1 ppkt 7, a także usuwania awarii, usterek, o których mowa w pkt. 2 ppkt 5 lit. b-c Zamawiający zastrzega sobie prawo do naliczenia kar umownych za zwłokę i potrącania ich z wynagrodzenia za realizowane wsparcie techniczne.

V. Rękojmia

Okres i warunki rękojmi:

1) Wykonawca udziela rękojmi na dostarczony System, do końca obowiązywania Umowy począwszy od dnia podpisania przez Strony bez zastrzeżeń Protokołu odbioru.
2) Zamawiający zastrzega sobie prawo dochodzenia roszczeń z tytułu rękojmi, zgodnie z przepisami Kodeksu cywilnego,
3) Informacje o wadach, Zamawiający będzie zgłaszał w dni robocze w godzinach 8:15-16:15, w formie pisemnej na adres poczty elektronicznej (e-mail) Wykonawcy.

VI. Zatrudnienie na podstawie stosunku pracy

1. Zamawiający wymaga, aby Wykonawca(y) lub Podwykonawca(y) w czasie realizacji Umowy zatrudniał(li) przynajmniej jedną osobę wykonującą czynności w zakresie przyjmowania zgłoszeń w ramach wsparcia technicznego, na podstawie stosunku pracy w rozumieniu przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277). Wykonawca(y) udokumentuje(ą) ten fakt poprzez złożenie dokumentów, o których mowa w ust. 3-4, na każde żądanie Zamawiającego.
2. Zamawiający wymaga, aby osoba, o której mowa w ust. 1, była zatrudniona przez cały okres realizacji Umowy przez Wykonawcę lub Podwykonawcę za wynagrodzeniem w wysokości nie mniejszej niż minimalne wynagrodzenie za pracę, w przeliczeniu na pełny etat, ustalone na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2024 r. poz. 1773).
3. W trakcie realizacji Umowy Zamawiający uprawniony jest do wykonywania czynności kontrolnych wobec Wykonawcy lub Podwykonawcy odnośnie spełniania przez Wykonawcę lub Podwykonawcę warunków opisanych w ust. 1 i 2, w szczególności do:
   1) żądania oświadczeń i dokumentów, o których mowa w ust. 4,
   2) żądania wyjaśnień w przypadku wątpliwości w zakresie potwierdzenia spełniania wymogów, o których mowa w ust. 1 i 2.
4. W trakcie realizacji Umowy, na każde wezwanie Zamawiającego, Wykonawca lub Podwykonawca przedłoży Zamawiającemu w celu potwierdzenia spełnienia wymogów, o których mowa w ust. 1 i 2, w terminie nie dłuższym niż 10 dni roboczych, od dnia przesłania przez Zamawiającego wezwania pisemnie lub za pośrednictwem poczty elektronicznej (e-mail), następujące dowody:
   1) oświadczenie Wykonawcy lub Podwykonawcy o zatrudnieniu na podstawie umowy o pracę osoby wskazanych w ust. 1, której dotyczy wezwanie Zamawiającego. Oświadczenie to powinno zawierać w szczególności: dokładne określenie podmiotu

składającego oświadczenie, datę złożenia oświadczenia, wskazanie, że objęte wezwaniem czynności wykonuje osoba zatrudniona na podstawie stosunku pracy wraz ze wskazaniem liczby tych osób, rodzaju stosunku pracy oraz podpis osoby uprawnionej do złożenia oświadczenia w imieniu Wykonawcy lub Podwykonawcy,

2) oświadczenie Wykonawcy lub Podwykonawcy o zatrudnieniu osób wykonujących czynności, o których mowa w ust. 1, za wynagrodzeniem w wysokości nie mniejszej niż minimalne wynagrodzenie za pracę ustalone na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę w przeliczeniu na pełny etat,
3) poświadczone za zgodność z oryginałem przez Wykonawcę lub Podwykonawcę kopię(e) umowy/umów o pracę osób wykonujących w trakcie realizacji Umowy czynności, których dotyczy ww. oświadczenie Wykonawcy. Kopie umów powinny zostać zanonimizowane w sposób zapewniający ochronę danych osobowych pracowników, tj. w szczególności bez adresów i nr PESEL pracowników. Imię i nazwisko pracownika nie podlega anonimizacji. Informacje takie jak: data zawarcia umowy, rodzaj umowy o pracę powinny być możliwe do zidentyfikowania,
4) zaświadczenie właściwego oddziału ZUS, potwierdzające opłacanie przez Wykonawcę składek na ubezpieczenia społeczne i zdrowotne z tytułu zatrudnienia na podstawie umów o pracę za ostatni okres rozliczeniowy – dotyczy pracowników, którzy kontynuują zatrudnienie u Wykonawcy lub Podwykonawcy,
5) poświadczoną za zgodność z oryginałem przez Wykonawcę lub Podwykonawcę kopię dowodu potwierdzającego zgłoszenie pracownika przez pracodawcę do ubezpieczeń, zanonimizowaną w sposób zapewniający ochronę danych osobowych pracowników, zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowychi w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. EU L z dnia 4 maja 2016 r., nr 119/1 z późn. zm.) imię i nazwisko pracownika nie podlega anonimizacji – dotyczy pracowników nowozatrudnionych przez Wykonawcę lub Podwykonawcę.

5. Niezłożenie przez Wykonawcę lub Podwykonawcę w wyznaczonym przez Zamawiającego terminie, nie dłuższym niż 10 dni roboczych, żądanych przez Zamawiającego dowodów, w celu potwierdzenia spełnienia przez Wykonawcę lub Podwykonawcę wymogu zatrudnienia na podstawie umowy o pracę traktowane będzie, jako niespełnienie przez Wykonawcę wymogu zatrudnienia na podstawie umowy o pracę osób wykonujących czynności wskazane w ust. 1 i stanowić będzie podstawę do naliczenia kar umownych, o których mowa w § 8 ust. 8 Umowy.
6. W przypadku rozwiązania stosunku pracy (bez względu na stronę składającą oświadczenie w tym zakresie) z osobą zatrudnioną/osobami zatrudnionymi na podstawie stosunku pracy, do wykonania czynności, o których mowa w ust. 1, przed zakończeniem realizacji Umowy, Wykonawca lub Podwykonawca zobowiązany jest do zatrudnienia na to miejsce innej(ych) osoby/osób w celu zagwarantowania realizacji przedmiotu Umowy zgodnie z wymaganiami Zamawiającego zawartymi w Opisie przedmiotu zamówienia, stanowiącym Załącznik nr 1 do Umowy.
7. W przypadku uzasadnionych wątpliwości, co do przestrzegania prawa pracy przez Wykonawcę lub Podwykonawcę, Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.
8. Za wszelkie działania i zaniechania osób skierowanych przez Wykonawcę lub Podwykonawcę do realizacji przedmiotu Umowy odpowiada wyłącznie Wykonawca.

VII. Informacje dodatkowe

1. Okres obowiązywania umowy wynosi … miesięcy (w zależności od złożonej oferty) od dnia jej zawarcia.
2. Wykonawca dostarczy serwery, urządzenia (o ile będą potrzebne), a także wdroży System i przekaże dokumentację powdrożeniową w terminie uzgodnionym z Zamawiającym jednak nie później niż …. miesiące (w zależności od złożonej oferty) od dnia zawarcia Umowy.